US009241261B2

(12) **United States Patent**
He

(10) **Patent No.: US 9,241,261 B2**
(45) **Date of Patent: *Jan. 19, 2016**

(54) METHOD, SYSTEM AND DEVICE FOR NEGOTIATING SECURITY CAPABILITY WHEN TERMINAL MOVES

(71) Applicant: **Huawei Technologies Co., Ltd.**, Shenzhen (CN)

(72) Inventor: **Chengdong He**, Shenzhen (CN)

(73) Assignee: **Huawei Technologies Co., Ltd.**, Shenzhen (CN)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/303,146**

(22) Filed: **Jun. 12, 2014**

(65) **Prior Publication Data**

US 2014/0295800 A1 Oct. 2, 2014

Related U.S. Application Data

(63) Continuation of application No. 14/147,179, filed on Jan. 3, 2014, now Pat. No. 8,812,848, which is a continuation of application No. 12/633,948, filed on Dec. 9, 2009, now Pat. No. 8,656,169, which is a continuation of application No. PCT/CN2008/072165, filed on Aug. 27, 2008.

(30) **Foreign Application Priority Data**

Aug. 31, 2007	(CN)	2007 1 0145703
Sep. 26, 2007	(CN)	2007 1 0151700

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04W 12/04	(2009.01)

(Continued)

(52) **U.S. Cl.**

CPC ***H04W 12/04*** (2013.01); ***H04L 9/088*** (2013.01); ***H04L 9/0844*** (2013.01);

(Continued)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,028,933 A *	2/2000	Heer	....	H04L 63/04 380/212
7,190,793 B2	3/2007	Hsu		

(Continued)

FOREIGN PATENT DOCUMENTS

CN	1455556 A	11/2003
CN	1710985 A	12/2005

(Continued)

OTHER PUBLICATIONS

Sargento, S.; Sarro, R.; Duarte, R.; Stupar, P.; Gallera, F.; Natkaniec, M.; Vilela, J.P.; Barros, J. Ubiquitous Access through the Integration of Mobile Ad-hoc Networks. 16th IST Mobile and Wireless Communications Summit. Pub. Date: 2007. Relevant pp. 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4299244.*

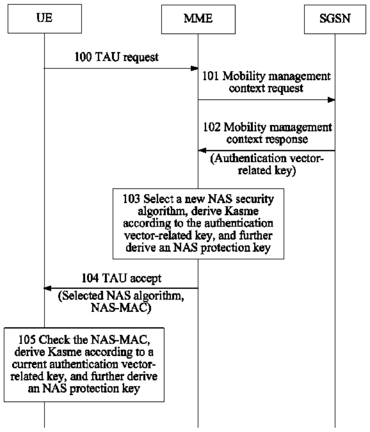
(Continued)

Primary Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Huawei Technologies Co., Ltd.

(57) ABSTRACT

An MME negotiates security in case of idle state mobility for a UE from a first network to a LTE network. The UE sends its security capabilities including non-access stratum (NAS) security capabilities supported by the UE to the LTE network. The MME selects a NAS security algorithm, in accordance with the NAS security capabilities of the UE, and sends the selected NAS security algorithm to the UE, sharing the NAS security algorithm between the UE and the LTE network when the UE moves from the first network to the LTE network. The MME also derives, in accordance with the selected NAS security algorithm, a NAS protection key from an authentication vector-related key so as to security communication between the UE and the LTE network.

24 Claims, 4 Drawing Sheets


UE
MME
SGSN
100 TAU request
101 Mobility management context request
102 Mobility management context response
(Authentication vector-related key)
103 Select a new NAS security algorithm, derive Kasme according to the authentication vector-related key, and further derive an NAS protection key
104 TAU accept
(Selected NAS algorithm, NAS-MAC)
105 Check the NAS-MAC, derive Kasme according to a current authentication vector-related key, and further derive an NAS protection key

(51) **Int. Cl.**

H04W 12/06	(2009.01)
H04L 9/08	(2006.01)
H04W 36/00	(2009.01)
H04W 12/12	(2009.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1441*** (2013.01); ***H04L 63/20*** (2013.01); ***H04L 63/205*** (2013.01); ***H04L 69/24*** (2013.01); ***H04W 12/06*** (2013.01); ***H04W 36/0038*** (2013.01); *H04L 2463/061* (2013.01); *H04W 12/12* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,929,703	B2 *	4/2011	Bellows	H04L 41/28 380/270
8,027,304	B2	9/2011	Forsberg	
8,078,753	B2 *	12/2011	Bachmann	H04W 8/04 370/255
8,107,433	B2 *	1/2012	Jokinen	H04W 36/0033 370/254
8,117,454	B2	2/2012	Forsberg	
8,165,054	B2 *	4/2012	Becker et al.	370/312
8,170,566	B2 *	5/2012	Pudney	455/445
8,213,903	B2	7/2012	Pudney et al.	
8,515,462	B2 *	8/2013	Courau	H04W 68/00 370/331
2002/0052200	A1 *	5/2002	Arkko et al.	455/432
2002/0071558	A1 *	6/2002	Patel	380/270
2003/0139180	A1 *	7/2003	McIntosh	H04L 63/0853 455/426.1
2006/0182280	A1 *	8/2006	Laitinen et al.	380/247
2007/0086591	A1 *	4/2007	Blom et al.	380/279
2007/0117575	A1 *	5/2007	Courau	H04W 68/00 455/458
2007/0218903	A1 *	9/2007	Grech	455/436
2007/0224993	A1	9/2007	Forsberg	
2007/0249352	A1 *	10/2007	Song	H04L 63/08 455/436
2007/0297367	A1 *	12/2007	Wang et al.	370/331
2008/0020745	A1 *	1/2008	Bae	H04W 60/04 455/422.1
2008/0025263	A1	1/2008	Pelkonen	
2008/0031159	A1 *	2/2008	Jokinen	H04W 36/0033 370/255
2008/0188200	A1 *	8/2008	Forsberg	455/410
2008/0207168	A1	8/2008	Forsberg	
2008/0301434	A1	12/2008	Haddad et al.	
2009/0067628	A1	3/2009	Pudney et al.	
2009/0275309	A1	11/2009	He	
2010/0235634	A1 *	9/2010	Fischer	H04L 63/0457 713/168
2014/0169563	A1	6/2014	Yan	

FOREIGN PATENT DOCUMENTS

CN	1801698	A	7/2006
CN	1983921	A	6/2007
EP	2214444	A1	8/2010
JP	2009531952	A	9/2009
JP	2009540721	A	11/2009
JP	2010521905	A	6/2010
JP	2010528559	A	8/2010
RU	2174924	C1	10/2001
WO	2007078159	A1	7/2007

OTHER PUBLICATIONS

Kim, Kyung-Ho. Key Technologies for the Next Generation Wireless Communications. Proceedings of the 4th International Conference Hardware/Software Codesign and System Synthesis, 2006. CODES+ISSS '06. Pub. Date: 2006. Relevant pp. 266-269. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4278527.*

R, Rajavelsamy; Jeedigunta, Venkateswar; Song, Osok. A Novel Method for Authentication Optimization during Handover in Heterogenous Wireless Networks. 2nd International Conference on Communication Systems Software and Middleware. Pub. Date: 2007. Relevant pp. 1-5. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4268139.*

Kueh, Victor Y.H.; Wilson, Mick. Application of Context Transfer for Roaming in IP-Based Evolved 3G Networks. 2006 IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications. Relevant pp. 1-5. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4022315.*

3GPP TS 23.401 V1.1.0; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; GPRS enhancements for E-UTRAN access (Release 8); Jul. 2007; total 77 pages.

3GPP TR 23.882 V1.11.0; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 7); Jul. 2007; total 211 pages.

3GPP TR 33.821 V0.4.0; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution(SAE) (Release 8); Jul. 2007; total 88 pages.

Nokia Siemens Networks, Nokia; Pseudo-CR to TR 33.821: Key handling on idle mode mobility; 3GPP TSG SA WG3 Security-S3-070529; Agenda Item: 6.14 SAE/LTE security, Jul. 10-13, 2007; Montreal, Canada; total 4 pages.

Huawei; Key handling on idle mode mobility form UTRAN to E-UTRAN; 3GPP TSG SA WG3 Security- 53#49; S3-070685; Agenda Item:6.14(SAE/LTE security); Oct. 8-12, 2007; Munich, Germany; total 2 pages.

3GPP TR 33.821 V0.2.0; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 8); Apr. 2007; total 78 pages.

3GPP TR 33.821 V0.3.0; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution(SAE) (Release 8); May 2007; total 84 pages.

A.R. Prasad, P. Schoo and H. Wang; An Evolutionary Approach towards Ubiquitous Communications: A Security Perspective; Saint 2004 Workshops. Pub. Date: 2004. Relevant pp. 689-695. Found on the World Wide Web at: http://ieeexplore.ieee.org/stannp/stamp.jsp?tp=&arnumber=1268719; total 7 pages.

Yeun, Chan Yeob; Lua, Eng Keong; Crowcroft, Jon; Security for Emerging Ubiquitous Networkd. IEEE 62nd Vehicular Technology Conference. vol. 2. Pub. Date: 2005; Relevant pp. 1242-1248; http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1558125; total 7 pages.

* cited by examiner

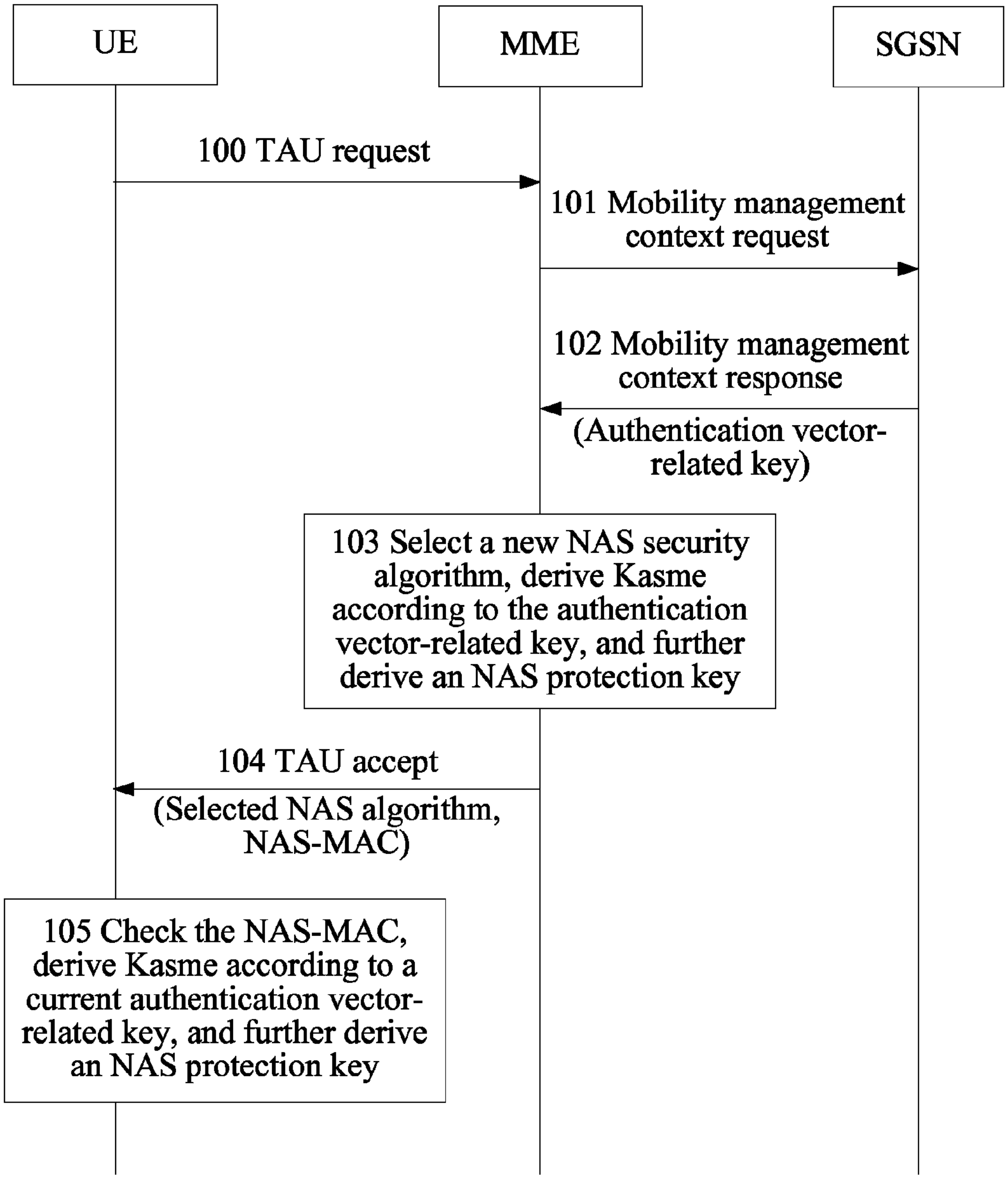

UE
MME
SGSN
100 TAU request
101 Mobility management context request
102 Mobility management context response
(Authentication vector-related key)
103 Select a new NAS security algorithm, derive Kasme according to the authentication vector-related key, and further derive an NAS protection key
104 TAU accept
(Selected NAS algorithm, NAS-MAC)
105 Check the NAS-MAC, derive Kasme according to a current authentication vector-related key, and further derive an NAS protection key

FIG. 1

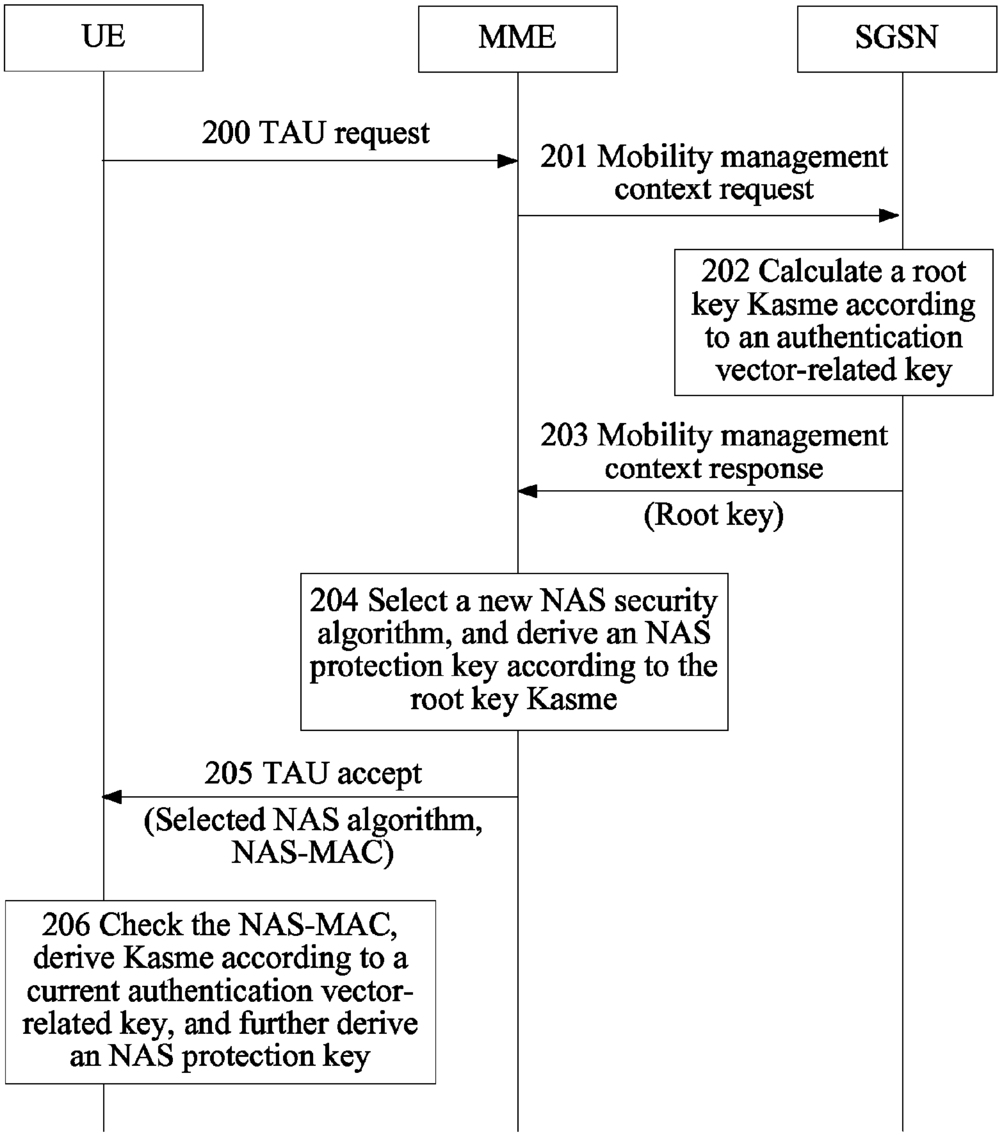

UE
MME
SGSN
200 TAU request
201 Mobility management context request
202 Calculate a root key Kasme according to an authentication vector-related key
203 Mobility management context response
(Root key)
204 Select a new NAS security algorithm, and derive an NAS protection key according to the root key Kasme
205 TAU accept
(Selected NAS algorithm, NAS-MAC)
206 Check the NAS-MAC, derive Kasme according to a current authentication vector-related key, and further derive an NAS protection key

FIG. 2

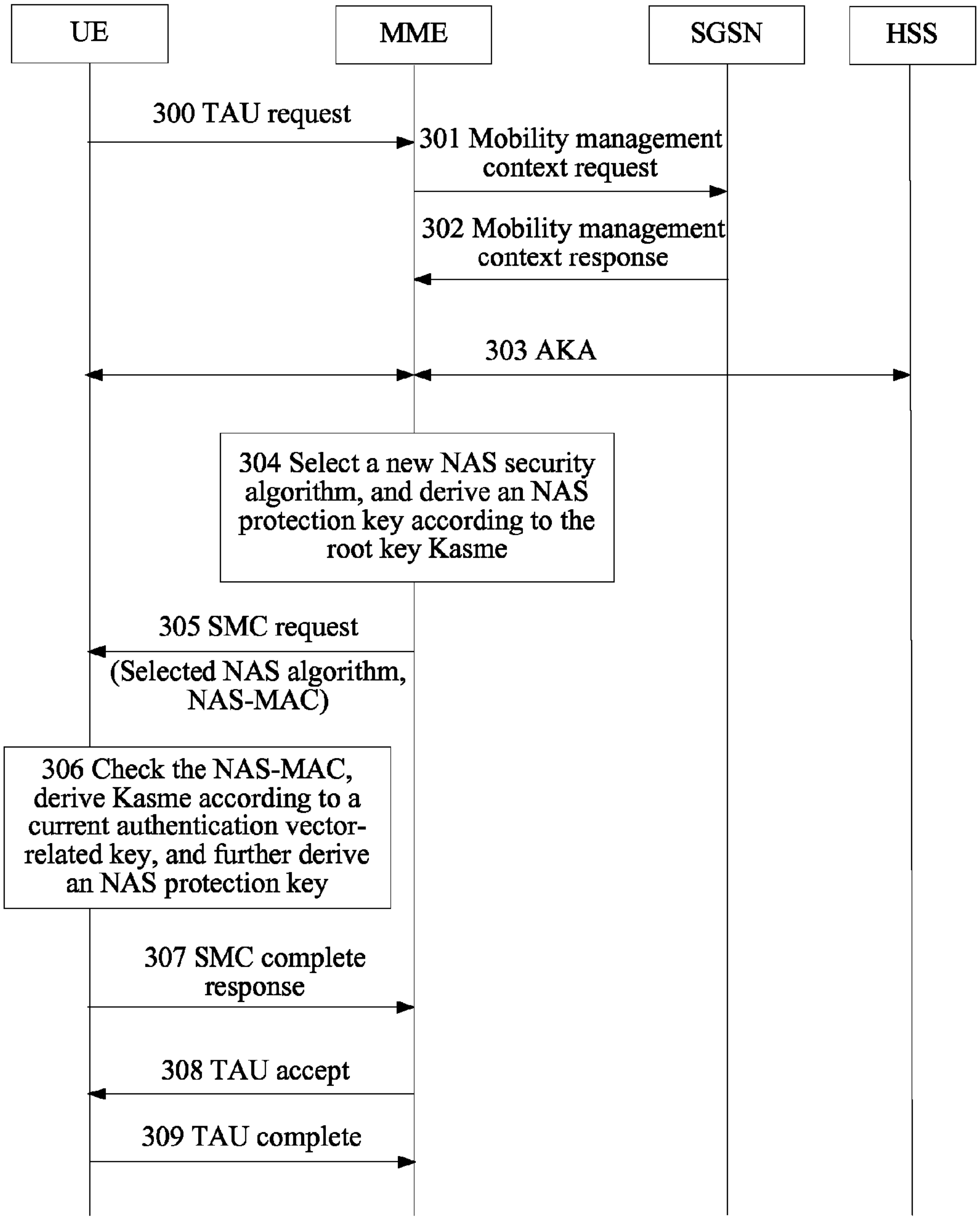

UE
MME
SGSN
HSS
300 TAU request
301 Mobility management context request
302 Mobility management context response
303 AKA
304 Select a new NAS security algorithm, and derive an NAS protection key according to the root key Kasme
305 SMC request
(Selected NAS algorithm, NAS-MAC)
306 Check the NAS-MAC, derive Kasme according to a current authentication vector-related key, and further derive an NAS protection key
307 SMC complete response
308 TAU accept
309 TAU complete

FIG. 3

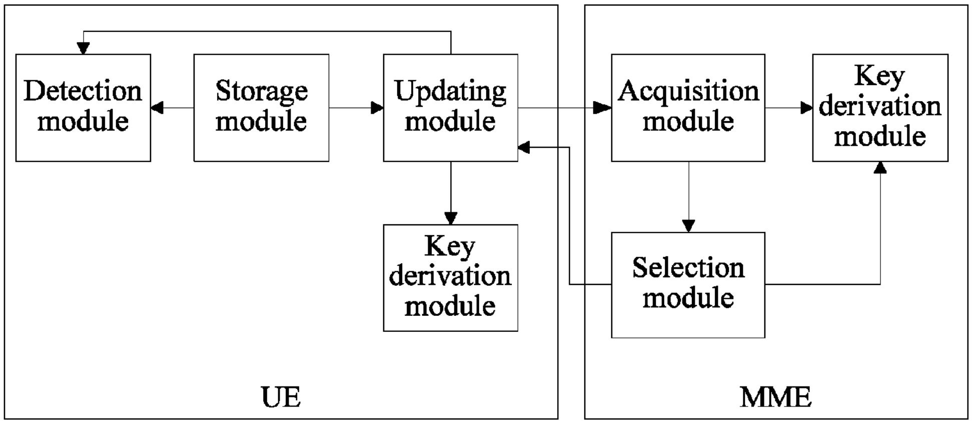

Detection module
Storage module
Updating module
Key derivation module
UE
Acquisition module
Key derivation module
Selection module
MME

FIG. 4

METHOD, SYSTEM AND DEVICE FOR NEGOTIATING SECURITY CAPABILITY WHEN TERMINAL MOVES

This application is a continuation of U.S. patent application Ser. No. 14/147,179, filed on Jan. 3, 2014, which is a continuation of U.S. patent application Ser. No. 12/633,948 (now U.S. Pat. No. 8,656,169), filed on Dec. 9, 2009, which is a continuation of International Application No. PCT/CN2008/072165, filed on Aug. 27, 2008, which claims priorities of Chinese Patent Application No. 200710145703.3, filed on Aug. 31, 2007 and Chinese Patent Application No. 200710151700.0, filed on Sep. 26, 2007, all of which are hereby incorporated by reference in their entireties.

TECHNICAL FIELD

The present invention relates to the field of wireless communication technology, and more particularly to a method and a system for negotiating a security capability when a terminal moves, a mobility management entity (MME), and a user equipment (UE).

BACKGROUND

A wireless network includes a radio access network and a core network. A core network of a long term evolution (LTE) wireless network includes an MME. The MME has functions similar to those of a service general packet radio service (GPRS) support node (SGSN) of a second/third generation (2G/3G) network, and is mainly responsible for mobility management and user authentication. When a UE is in an idle state in a 2G/3G or LTE wireless network, the UE needs to respectively negotiate a non-access stratum (NAS) security capability with the SGSN or the MME. The security capability includes an NAS signaling encryption algorithm, a corresponding NAS integrity protection key Knas-int, an NAS integrity protection algorithm, and a corresponding NAS confidentiality protection key Knas-enc, which are used for signaling transmission between the UE and a system, thereby ensuring the normal receiving of the UE signaling and the security of the communication system.

When the UE accessing a 2G global system for mobile communications (GSM) edge radio access network (GERAN) or a 3G universal mobile telecommunications system (UMTS) terrestrial radio access network (UTRAN) moves in the idle state, the UE may move to a tracking area of an LTE radio access network, and thus the UE may access the network again through the LTE. At this time, a tracking area update (TAU) procedure occurs, that is, a TAU procedure between heterogeneous networks occurs. During the procedure, since the entity performing security capability negotiation for the UE changes, for example, from the SGSN to the MME, and the entities may have different security capabilities, the security capability negotiation procedure needs to be performed again, so as to ensure the security of subsequent interaction between the UE and the network. It should be noted that, for the LTE network, the security capability negotiation includes negotiation of an NAS confidentiality protection algorithm and an NAS integrity protection algorithm, a radio resource control (RRC) confidentiality protection algorithm and an RRC integrity protection algorithm, and a user plane (UP) confidentiality protection algorithm.

For the TAU procedure initiated by the UE in the idle state, the negotiation of the NAS confidentiality protection algorithm, the NAS integrity protection algorithm, and the corresponding NAS protection keys need to be solved.

During the implementation of the present invention, the inventor found that, no method for negotiating the security capability during the TAU procedure between the heterogeneous networks can be found in the prior art, so that when the UE moves from the 2G/3G network to the LTE network, the security capability negotiation cannot be performed, resulting in that the security of subsequent interaction between the UE and the network cannot be ensured.

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a method for negotiating a security capability when a terminal moves, so that when moving from a 2G/3G network to an LTE network, a UE in an idle state can negotiate a security capability.

The present invention is further directed to a system for negotiating a security capability when a terminal moves, so that when moving from a 2G/3G network to an LTE network, a UE in an idle state can negotiate a security capability.

The present invention is further directed to an MME, so that when moving from a 2G/3G network to an LTE network, a UE in an idle state can negotiate a security capability.

The present invention is further directed to a UE device, so that when moving from a 2G/3G network to an LTE network, a UE in an idle state can negotiate a security capability.

In order to achieve the objectives, technical solutions of the present invention are implemented as follows.

A method for negotiating a security capability when a terminal moves is provided, which includes the following steps.

An MME receives a TAU request message sent from a UE, and acquires an NAS security algorithm supported by the UE, and an authentication vector-related key or a root key derived according to the authentication vector-related key.

The MME selects an NAS security algorithm according to the NAS security algorithm supported by the UE, derives an NAS protection key according to the authentication vector-related key or the root key, and sends a message carrying the selected NAS security algorithm to the UE.

The UE derives an NAS protection key according to an authentication vector-related key thereof.

A system for negotiating a security capability when a terminal moves is provided, which includes a UE and an MME.

The UE is adapted to send a TAU request message to the MME, receive a message carrying a selected NAS security algorithm sent from the MME, and derive an NAS protection key according to an authentication vector-related key.

The MME is adapted to: receive the TAU request message sent from the UE; acquire an authentication vector-related key or a root key derived according to the authentication vector-related key, and an NAS security algorithm supported by the UE; select an NAS security algorithm according to the NAS security algorithm supported by the UE, and generate and send a message carrying the selected NAS security algorithm to the UE; and derive an NAS protection key according to the acquired authentication vector-related key or the root key.

An MME is provided, which includes an acquisition module, a selection module, and a key derivation module.

The acquisition module is adapted to receive a TAU request message sent from a UE, acquire an authentication vector-related key or a root key derived according to the authentication vector-related key, and an NAS security algorithm supported by the UE.

The selection module is adapted to select an NAS security algorithm according to the NAS security algorithm supported by the UE and acquired by the acquisition module, generate a message carrying the selected NAS security algorithm, and send the message to the UE.

The key derivation module is adapted to derive an NAS protection key according to the authentication vector-related key or the root key derived according to the authentication vector-related key acquired by the acquisition module, and the NAS security algorithm selected by the selection module.

A UE is provided, which includes an updating module, a key derivation module, a storage module, and a detection module.

The updating module is adapted to send to an MME a TAU request message carrying security capability information supported by the UE and stored in the storage module, and receive a message carrying a selected NAS security algorithm sent from the MME.

The key derivation module is adapted to derive an NAS protection key according to an authentication vector-related key and the NAS security algorithm received by the updating module.

The storage module is adapted to store the security capability information supported by the UE.

The detection module is adapted to determine that a degradation attack occurs when detecting that security capability information supported by the UE and received from the MME is inconsistent with the security capability information supported by the UE and stored in the storage module.

A method for negotiating a security capability when a terminal moves, wherein when a user equipment (UE) moves from a second/third generation (2G/3G) network to a long term evolution (LTE) network, the method comprises:

receiving, by a mobility management entity (MME), a tracking area update (TAU) request message sent from the UE, and acquiring a non-access signaling (NAS) security algorithm supported by the UE, and an authentication vector-related key or a root key derived according to the authentication vector-related key;

selecting, by the MME, an NAS security algorithm according to the NAS security algorithm supported by the UE, deriving an NAS protection key according to the authentication vector-related key or the root key, and sending a message carrying the selected NAS security algorithm to the UE.

In the technical solutions of the present invention, the MME receives the TAU request message sent from the UE, and acquires the authentication vector-related key or the root key derived according to the authentication vector-related key and the NAS security algorithm supported by the UE; then selects the NAS security algorithm according to the NAS security algorithm supported by the UE, generates a message carrying the selected NAS security algorithm, and sends the message to the UE, thereby enabling the UE and the MME to share the NAS security algorithm. In addition, the MME derives the NAS protection key according to the authentication vector-related key or the root key derived according to the authentication vector-related key, and the UE derives the NAS protection key according to the authentication vector-related key, thereby enabling the MME and the UE to share the NAS protection key. In this way, when moving from the 2G/3G network to the LTE network, the UE can negotiate the NAS security algorithm and the NAS protection key with the MME, so that the security capability negotiation process in the TAU procedure between heterogeneous networks is achieved, thereby ensuring the security of subsequent interaction between the UE and the network.

In addition, the present invention is also applicable to a security capability negotiation procedure when the UE moves within the LTE network.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a flow chart of a method, according to a first embodiment of the present invention, for negotiating a security capability when a terminal moves;

FIG. **2** is a flow chart of a method, according to a second embodiment of the present invention, for negotiating a security capability when a terminal moves;

FIG. **3** is a flow chart of a method, according to a third embodiment of the present invention, for negotiating a security capability when a terminal moves; and

FIG. **4** is a structural view of a system, according to an embodiment of the present invention, for negotiating a security capability when a terminal moves.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

In a method for negotiating a security capability when a terminal moves provided in the embodiments of the present invention, when a UE moves from a 2G/3G network to an LTE network, an MME receives a TAU request message sent from the UE, and acquires an NAS security algorithm supported by the UE, and an authentication vector-related key or a root key derived according to the authentication vector-related key. Then, the MME selects an NAS security algorithm according to the NAS security algorithm supported by the UE, derives an NAS protection key according to the authentication vector-related key or the root key derived according to the authentication vector-related key, and sends a message carrying the selected NAS security algorithm to the UE. The UE derives an NAS protection key according to an authentication vector-related key.

The embodiments of the present invention are illustrated in detail below with reference to specific embodiments and the accompanying drawings.

It is assumed that a UE has accessed a UTRAN/GERAN when being in an idle state. In this case, when moving to a tracking area of an LTE network, the UE initiates a TAU procedure.

FIG. **1** is a flow chart of a method, according to a first embodiment of the present invention, for negotiating a security capability when a terminal moves. Referring to FIG. **1**, the method includes the following steps.

In step **100**, a UE sends a TAU request to an MME.

In this step, the UE sends the TAU request to a new MME through an evolved Node B (eNB) of an LTE radio access network. For the convenience of description, communication between the UE and the MME through the eNB is simplified to communication between the UE and the MME in the following description.

The TAU request sent from the UE to the MME in this step not only carries some parameters such as a temporary mobile subscriber identity (TMSI) known to persons skilled in the art, but may also carry security capability information supported by the UE. The security capability information includes an NAS security algorithm (an NAS integrity protection algorithm and/or an NAS confidentiality protection algorithm), and may also include an RRC security algorithm (an RRC integrity protection algorithm and/or an RRC confidentiality protection algorithm) or a UP security algorithm (a UP confidentiality protection algorithm).

In steps **101**-**102**, the MME acquires an NAS security algorithm supported by the UE, and sends a mobility management context request message to an SGSN. After receiving the message, the SGSN sends a mobility management context response message carrying an authentication vector-related key to the MME.

If in step **100**, the UE does not carry the NAS security algorithm supported by the UE in the TAU request sent to the MME, after receiving the mobility management context request message, the SGSN queries the NAS security algorithm supported by the UE, and carries the queried NAS security algorithm supported by the UE in the mobility management context response message sent to the MME. The NAS security algorithm is the NAS integrity protection algorithm and/or the NAS confidentiality protection algorithm.

When the UE moves from the 2G network to the tracking area of the LTE network, the SGSN in the above process is an SGSN of the 2G network, and the authentication vector-related key at least includes an encryption key Kc, or a value Kc' obtained after a unidirectional conversion is performed on the Kc. When the UE moves from the 3G network to the tracking area of the LTE network, the SGSN in the above process is an SGSN of the 3G network, and the authentication vector-related key at least includes an integrity key IK and an encryption key CK, or values IK' and CK' after a unidirectional conversion is performed on the IK and the CK.

The unidirectional conversion refers to a conversion procedure in which an original parameter is converted by using a certain algorithm to obtain a target parameter, but the original parameter cannot be derived according to the target parameter. For example, for the Kc, if the Kc' is obtained by using an algorithm f(Kc), but the Kc cannot be derived according to the Kc' by using any inverse algorithm, the conversion is the unidirectional conversion.

In step **103**, the MME selects a new NAS security algorithm, according to the NAS security algorithm supported by the UE and an NAS security algorithm supported by the MME as well as an NAS security algorithm allowed by the system, derives a root key Kasme according to the authentication vector-related key, and then derives an NAS protection key according to the Kasme. The NAS protection key includes an NAS integrity protection key Knas-int and/or an NAS confidentiality protection key Knas-enc.

In step **104**, the MME generates a TAU accept message carrying the selected NAS security algorithm.

In this step, the MME may further perform an NAS integrity protection on the TAU accept message. For example, the MME derives a value of a message authentication code of the NAS integrity protection (NAS-MAC) according to the NAS integrity protection key Knas-int derived in step **103**, information in the TAU accept, and the NAS integrity protection algorithm in the selected NAS security algorithm, and then carries the value in the TAU accept message, and sends the TAU accept message to the UE.

The TAU accept message in this step may further carry security capability information supported by the UE.

In step **105**, the UE receives the TAU accept message carrying the NAS security algorithm selected by the MME, and acquires the negotiated NAS security algorithm; and then derives a root key Kasme according to a current authentication vector-related key thereof (for example, the IK and the CK, or the IK' and the CK' derived according to the IK and the CK when the originating network is the 3G, or the Kc or the Kc' derived according to the Kc when the originating network is the 2G), and derives an NAS protection key according to the root key. The NAS protection key includes the NAS integrity protection key Knas-int and/or the NAS confidentiality protection key Knas-enc.

In this step, the UE may further detect whether the integrity protection performed on the TAU accept message is correct. If not, it is determined that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again. For example, the UE derives an NAS-MAC according to the derived NAS confidentiality protection key Knas-enc, the information in the TAU accept, and the NAS integrity protection algorithm carried in the TAU accept message, and then compares whether the derived NAS-MAC is the same as the NAS-MAC carried in the TAU accept message. If yes, it indicates that the message is not modified during transmission; otherwise, it is deemed that the message is modified during transmission, and it is thus determined that the current security capability negotiation fails.

If in step **104**, the TAU accept message further carries the security capability information supported by the UE, in this step, the UE may further compare the security capability information supported by the UE and carried in the TAU accept message with security capability information stored therein. If the two are consistent with each other, it is determined that no degradation attack occurs; otherwise, it is determined that a degradation attack occurs, and that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again, thereby preventing the degradation attack.

For the degradation attack, it is assumed that the UE supports two security algorithms at the same time, namely, a high strength algorithm A**1** and a low strength algorithm A**2**, and the MME also supports the two algorithms. In this manner, the high strength algorithm A**1** should be negotiated between the UE and the MME. However, if in a path along which the UE sends the security capability information supported by the UE to the MME, an attacker modifies the security capability information of the UE, for example, only the low strength algorithm A**2** is maintained, or when the MME selects the NAS security algorithm, the security capability information supported by the UE is modified by the attacker, and only the low strength algorithm A**2** is maintained, the MME can only select and send the low strength algorithm A**2** to the UE. That is, the low strength algorithm A**2**, rather than the high strength algorithm A**1**, is obtained through the negotiation between the UE and the MME, so that the attacker may perform an attack more easily, which is the so-called degradation attack. In an embodiment of the present invention, the MME sends the security capability information supported by the UE to the UE, and the UE detects whether the security capability information supported by the UE is consistent with the security capability information supported by the UE, thereby detecting and further preventing the degradation attack.

The procedure that the MME finally derives the NAS protection key according to the authentication vector-related key in step **103** is not limited to any time sequence with respect to step **104** and step **105**, and the procedure may be performed before step **104**, or between step **104** and step **105**, or after step **105**.

In the above process, the MME and the UE may also directly derive the NAS protection key according to the authentication vector-related key without deriving the root key and then deriving the NAS protection key according to the root key.

It should be understood by persons skilled in the art that, in the above process, a derivation method used by the UE to derive the NAS protection key according to the authentication vector-related key must be the same as that used by the network side to derive the NAS protection key according to the authentication vector-related key. The derivation method may adopt any unidirectional conversion, for example, Kasme=f (IK, CK, other parameters), Knas-enc=f(Kasme, NAS confidentiality protection algorithm, other parameters), and Knas-int=f (Kasme, NAS integrity protection algorithm, other parameters).

In addition, in order to highlight this embodiment of the present invention, procedures that are not related to the security are omitted between steps **102** and **104** in the above process.

Through the above process, the UE and the MME can share the NAS security algorithm and the NAS protection key, thereby implementing the negotiation of the NAS security capability.

FIG. **2** is a flow chart of a method, according to a second embodiment of the present invention, for negotiating a security capability when a terminal moves. Referring to FIG. **2**, the method includes the following steps.

Step **200** is the same as step **100**, so description thereof is omitted here.

In steps **201**-**203**, the MME acquires an NAS security algorithm supported by the UE, and sends a context request message to an SGSN. After receiving the context request message, the SGSN derives a root key according to an authentication vector-related key thereof, and then sends a context response message carrying the root key to the MME.

In other embodiments of the present invention, if in step **200**, the UE does not carry the NAS security algorithm supported by the UE in the TAU request sent to the MME, after receiving the mobility management context request message, the SGSN queries the NAS security algorithm supported by the UE, and carries the queried NAS security algorithm supported by the UE in the mobility management context response message sent to the MME. The NAS security algorithm is the NAS integrity protection algorithm and/or the NAS confidentiality protection algorithm.

When the UE moves from the 2G network to the tracking area of the LTE network, the SGSN in the above process is an SGSN of the 2G network, and the root key is the root key Kasme derived by the SGSN according to the Kc or the Kc' obtained after the unidirectional conversion is performed on the Kc. When the UE moves from the 3G network to the tracking area of the LTE network, the SGSN in the above process is an SGSN of the 3G network, and the root key is the Kasme derived by the SGSN according to the IK and the CK, or the IK' and the CK' after the unidirectional conversion is performed on the IK and the CK.

In step **204**, the MME selects a new NAS security algorithm, according to the NAS security algorithm supported by the UE and an NAS security algorithm supported by the MME as well as an NAS security algorithm allowed by the system; and then derives an NAS protection key according to the root key. The NAS protection key includes an NAS integrity protection key Knas-int and/or an NAS confidentiality protection key Knas-enc.

In step **205**, the MME generates a TAU accept message carrying the selected NAS security algorithm.

In this step, the MME may further perform an NAS integrity protection on the TAU accept message. The TAU accept message in this step may further carry security capability information supported by the UE.

In step **206**, the UE receives the TAU accept message carrying the NAS security algorithm selected by the MME, and acquires the negotiated NAS security algorithm; and then derives a root key Kasme according to a current authentication vector-related key (for example, the IK and the CK, or the IK' and the CK' derived according to the IK and the CK when the originating network is the 3G, or the Kc or the Kc' derived according to the Kc when the originating network is the 2G), and derives an NAS protection key according to the root key. The NAS protection key includes the NAS integrity protection key Knas-int and/or the NAS confidentiality protection key Knas-enc.

In this step, the UE may further detect whether the integrity protection performed on the TAU accept message is correct. If not, it is determined that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again.

In other embodiments of the present invention, if in step **205**, the TAU accept message further carries the security capability information supported by the UE, in this step, the UE may further compare the security capability information supported by the UE carried in the TAU accept message with security capability information supported by the UE. If the two are consistent with each other, it is determined that no degradation attack occurs; otherwise, it is determined that a degradation attack occurs, and that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again, thereby preventing the degradation attack.

In other embodiments of the present invention, the procedure that the MME derives the NAS protection key according to the root key in step **204** is not limited to any time sequence with respect to step **205** and step **206**, and the procedure may be performed before step **205**, or between step **205** and step **206**, or after step **206**.

It should be understood by persons skilled in the art that, in the above process, a derivation method used by the UE to derive the NAS protection key according to the authentication vector-related key must be the same as that used by the network side to derive the NAS protection key according to the authentication vector-related key.

Through the above process, the UE and the MME can share the NAS security algorithm and the NAS protection key, thereby implementing the negotiation of the NAS security capability.

FIG. **3** is a flow chart of a method, according to a third embodiment of the present invention, for negotiating a security capability when a terminal moves. Referring to FIG. **3**, the method includes the following steps.

Step **300** is the same as step **100**, so description thereof is omitted here.

In steps **301**-**302**, the MME acquires an NAS security algorithm supported by the UE from an SGSN through mobility management context request and response messages.

In other embodiments of the present invention, if in step **300**, the UE does not carry the NAS security algorithm supported by the UE in the TAU request sent to the MME, after receiving the mobility management context request message, the SGSN queries the NAS security algorithm supported by the UE, and carries the queried NAS security algorithm supported by the UE in the mobility management context response message sent to the MME. The NAS security algorithm is the NAS integrity protection algorithm and/or the NAS confidentiality protection algorithm.

In step **303**, the MME acquires a root key Kasme derived according to an authentication vector-related key from a home subscriber server (HSS) through an authentication and key agreement (AKA) procedure.

In step **304**, the MME selects a new NAS security algorithm , according to the NAS security algorithm supported by the UE and an NAS security algorithm supported by the MME as well as and an NAS security algorithm allowed by the system; and then derives other NAS protection keys according to the Kasme. The NAS protection keys include an NAS integrity protection key Knas-int and an NAS confidentiality protection key Knas-enc.

In step **305**, the MME generates and sends to the UE an NAS security mode command (SMC) request message carrying the selected NAS security algorithm. The SMC request message may be carried in a TAU accept message.

In this step, the MME may further perform an NAS integrity protection on the SMC accept message. For example, the MME derives a value of an message authentication code of the NAS integrity protection (NAS-MAC) according to the NAS integrity protection key Knas-int derived in step **304**, information in the SMC request message, and the NAS integrity protection algorithm in the selected NAS security algorithm, and then carries the value in the SMC request message, and sends the SMC request message to the UE.

The SMC request message in this step may further carry security capability information supported by the UE.

In step **306**, the UE receives the SMC request message carrying the NAS security algorithm selected by the MME, and acquires the NAS security algorithm supported by the UE and selected by the MME; and then derives a root key according to a current authentication vector-related key obtained in an AKA procedure thereof, and derives an NAS protection key according to the root key. The NAS protection key includes the NAS integrity protection key Knas-int and the NAS confidentiality protection key Knas-enc.

In this embodiment, in this step, the UE may further detect whether the integrity protection performed on the TAU accept message is correct. If not, it is determined that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again. For example, the UE derives an NAS-MAC according to the derived NAS confidentiality protection key Knas-enc, the information in the TAU accept message, and the NAS integrity protection algorithm carried in the TAU accept message, and then compares whether the derived NAS-MAC is the same as the NAS-MAC carried in the TAU accept message. If yes, it indicates that the message is not modified during transmission; otherwise, it is deemed that the message is modified during transmission, and it is thus determined that the current security capability negotiation fails.

In other embodiments of the present invention, if in step **305**, the SMC request message further carries the security capability information supported by the UE, in this step, the UE may further compare the security capability information supported by the UE and carried in the SMC request message with security capability information supported by the UE. If the two are consistent with each other, it is determined that no degradation attack occurs; otherwise, it is determined that a degradation attack occurs, and that the current security capability negotiation fails, and the security capability negotiation procedure may be initiated again, thereby preventing the degradation attack.

In step **307**, the UE sends an SMC complete response message to the MME. The SMC complete response message may be carried in a TAU complete message.

In step **308**, the MME returns a TAU accept message.

In other embodiments of the present invention, when the SMC request message is sent to the UE by carrying the SMC request message in the TAU accept message in step **305**, step **308** is combined with step **305**.

In step **309**, the UE returns a TAU complete message.

In other embodiments of the present invention, when the SMC complete response message is carried in the TAU complete message in step **307**, step **309** is combined with step **307**.

Through the above process, the negotiation of the NAS security capability is implemented.

Persons of ordinary skill in the art should understand that all or a part of the steps in the method according to the embodiments of the present invention may be implemented by a program instructing relevant hardware, and the program may be stored in a computer readable storage medium, such as a read-only memory (ROM)/random access memory (RAM), a magnetic disk, or an optical disk.

FIG. **4** is a structural view of a system, according to an embodiment of the present invention, for negotiating a security capability when a terminal moves. Referring to FIG. **4**, the system includes a UE and an MME.

The UE is adapted to send a TAU request message to the MME, receive a message carrying a selected NAS security algorithm sent from the MME, and derive an NAS protection key according to an authentication vector-related key.

The MME is adapted to: receive the TAU request message sent from the UE; acquire an authentication vector-related key or a root key derived according to the authentication vector-related key, and an NAS security algorithm supported by the UE; select an NAS security algorithm according to the NAS security algorithm supported by the UE, and generate and send a message carrying the selected NAS security algorithm to the UE; and derive an NAS protection key according to the acquired authentication vector-related key or the root key derived according to the authentication vector-related key.

In the system, the MME further acquires security capability information supported by the UE, and further carries the security capability information supported by the UE in the message carrying the selected NAS security algorithm sent to the UE, and the UE further determines whether a degradation attack occurs by determining whether the security capability information supported by the UE and sent from the MME is consistent with security capability information supported by the UE.

Specifically, the MME includes an acquisition module, a selection module, and a key derivation module.

The acquisition module is adapted to receive the TAU request message sent from the UE, acquire the authentication vector-related key or the root key derived according to the authentication vector-related key, and the NAS security algorithm supported by the UE. The selection module is adapted to select the NAS security algorithm according to the NAS security algorithm supported by the UE and acquired by the acquisition module, generate and send the message carrying the selected NAS security algorithm to the UE. The key derivation module is adapted to derive the NAS protection key, according to the authentication vector-related key or the root key derived according to the authentication vector-related key acquired by the acquisition module, and the selected NAS security algorithm.

The acquisition module further acquires the security capability information supported by the UE, and the selection module further carries the security capability information supported by the UE and acquired by the acquisition module in the message carrying the selected NAS security algorithm.

The UE includes an updating module, a key derivation module, a storage module, and a detection module.

The updating module is adapted to send the TAU request message carrying the security capability information supported by the UE and stored in the storage module to the MME, and receive the message carrying the selected NAS security algorithm sent from the MME. The key derivation module is adapted to derive the NAS protection key according to the authentication vector-related key and the selected NAS security algorithm received by the updating module. The storage module is adapted to store the security capability information supported by the UE. The detection module is adapted to determine that a degradation attack occurs when detecting that the security capability information supported by the UE and received from the MME is inconsistent with the security capability information supported by the UE and stored in the storage module. The message carrying the selected NAS security algorithm sent from the MME further carries security capability information supported by the UE.

It can be seen from the above description that, in the technical solutions provided in embodiments of the present invention, the MME receives the TAU request message sent from the UE, and acquires the NAS security algorithm supported by the UE and the authentication vector-related key or the root key derived according to the authentication vector-related key; and then selects the NAS security algorithm according to the NAS security algorithm supported by the UE, and generates and sends the message carrying the selected NAS security algorithm to the UE, thereby enabling the UE and the MME to share the NAS security algorithm. In addition, the UE and the MME derive the NAS protection key according to the authentication vector-related key or the root key derived according to the authentication vector-related key, thereby enabling the MME and the UE to share the NAS protection key. In this way, when moving from the 2G/3G network to the LTE network, the UE can negotiate the NAS security algorithm and the NAS protection key with the MME, so that the security capability negotiation process in the TAU procedure between the heterogeneous networks is achieved, thereby ensuring the security of subsequent interaction between the UE and the network.

Through the present invention, the degradation attack can be further prevented. The MME also returns the security capability information supported by the UE through the TAU accept message, and the UE detects whether the security capability information supported by the UE is consistent with the current security capability information supported by the UE. If yes, the current security capability negotiation succeeds, and the NAS security algorithm and the NAS protection key obtained through the negotiation can be used. If not, it is determined that a degradation attack occurs, the current security capability negotiation fails, and the security capability negotiation needs to be performed again. Through the above solutions, it can be detected whether the security capability information supported by the UE is attacked before the MME acquires the security capability information supported by the UE, thereby preventing the degradation attack and ensuring the security of subsequent interaction between the UE and the network.

The above descriptions are merely preferred embodiments of the present invention, but not intended to limit the protection scope of the present invention. Any modification, equivalent replacement, and improvement made without departing from the spirit and principle of the present invention fall within the protection scope of the present invention.

What is claimed is:

1. A method of security negotiation for idle state mobility from a first network to a long term evolution (LTE) network using a mobility management entity (MME), the method comprising:

transmitting an authentication vector-related key from a service general packet radio service (GPRS) support node (SGSN) in the first network to the MME;

receiving security capabilities of a user equipment (UE) including non-access stratum (NAS) security capabilities of the UE from the UE;

selecting a NAS security algorithm supported by the NAS security capabilities of the UE;

sending a message that indicates the selected NAS security algorithm to the UE; and deriving a NAS protection key with the selected NAS security algorithm from the authentication vector-related key.

2. The method of claim **1**, wherein the security capabilities is received in a tracking area update (TAU) request message.

3. The method of claim **1**, wherein the message that indicates the selected NAS security algorithm is one of NAS security mode command message and a tracking area update (TAU) accept message.

4. The method of claim **1**, further comprising, before the sending, the message that indicates the selected NAS security algorithm:

protecting the message that indicates the selected NAS security algorithm, with the derived NAS protection key.

5. The method of claim **1**, wherein the first network is one of a second generation (2G) network, a third generation (3G) network and a second LTE network.

6. The method of claim **1**, wherein the first network is a second generation (2G) network and the authentication vector-related key includes an encryption key (Kc).

7. The method of claim **1**, wherein the first network is a third generation (3G) network and the authentication vector-related key includes an integrity key (IK) and an encryption key (CK).

8. The method of claim **1** wherein the authentication vector-related key is transmitted through a context response message.

9. A communications system comprising:

an acquisition module that receives from a user equipment (UE) security capabilities of the UE including non-access stratum (NAS) security capabilities of the UE;

a service general packet radio service (GPRS) support node (SGSN) in a first network that sends an authentication vector-related key to the acquisition module;

a selection module that selects a NAS security algorithm supported by the NAS security capabilities of the UE and sends a message that indicates the selected NAS security algorithm to the UE; and

a key derivation module that derives a NAS protection key with the selected NAS security algorithm from the authentication vector-related key, wherein the communications system provides security negotiation for idle state mobility from the first network to a long term evolution (LTE) network;

wherein the acquisition module, the selection module and the key derivation module are included in a mobility management entity (MME).

10. The communications system of claim **9**, wherein security capabilities of the UE is received in a tracking area update (TAU) request message.

11. The communications system of claim **9**, wherein the message that indicates the selected NAS security algorithm is one of a NAS security mode command message and a tracking area update (TAU) accept message.

12. The communications system of claim **9**, wherein at least one of the modules in the system further protects the message that indicates the selected NAS security algorithm with the derived NAS protection key.

13. The communications system of claim **9**, wherein the first network is one of a second generation (2G) network, a third generation (3G) network, and a second LTE network.

14. The communications system of claim **9**, wherein the first network is a second generation (2G) network and the authentication vector-related key includes an encryption key (Kc).

15. The communications system of claim **9**, wherein the first network is a third generation (3G) network and the authentication vector-related key includes an integrity key (IK) and an encryption key (CK).

16. The communications system of claim **9**, wherein the authentication vector-related key is sent through a context response message.

17. A communications system that provides security negotiation for idle state mobility from a first network to a long term evolution (LTE) network comprising:

a mobility management entity (MME) that receives security capabilities of a user equipment (UE) including non-access stratum (NAS) security capabilities of a UE from the UE; and

a service general packet radio service (GPRS) support node (SGSN) in the first network that sends an authentication vector-related key to the MME,

wherein the MME is in the LTE network and

selects a NAS security algorithm supported by the NAS security capabilities of the UE,

sends a message that indicates the selected NAS security algorithm to the UE, and

derives a NAS protection key with the selected NAS security algorithm from the authentication vector-related key.

18. The communications system of claim **17**, wherein the MME receives the security capabilities in a tracking area update (TAU) request message.

19. The communications system of claim **17**, wherein the message that indicates the selected NAS security algorithm is one of a NAS security mode command message and a tracking area update (TAU) accept message.

20. The communications system of claim **17**, wherein the MME further protects the message that indicates the selected NAS security algorithm with the derived NAS protection key.

21. The communications system of claim **17**, wherein the first network is one of a second generation (**2**G) network, a third generation (**3**G) network, and a second LTE network.

22. The communications system of claim **17**, wherein the first network is a second generation (**2**G) network and the authentication vector-related key includes an encryption key (Kc).

23. The communications system of claim **17**, wherein the first network is a third generation (**3**G) network and the authentication vector-related key includes an integrity key (IK) and an encryption key (CK).

24. The communications system of claim **17**, wherein the SGSN sends the authentication vector-related key through a context response message.

* * * * *